Claims pending: 1-8 and 36-58

Canceled or Withdrawn claims: Claims 9-35 were previously canceled

Amended claim(s): 1-7

5   **New claims:** 36-58

This listing of claims replaces all prior versions and listings:

1.   (Currently Amended)   A   pseudonymous   email   address

10   generator ~~for generating a pseudonymous email address associated with an email~~

~~address, the generator~~ comprising:

a   request   interface[[,]]   <u>configured to</u>   [[for receiving]]   <u>receive</u>   a

pseudonymous   email   address   generation   request   [[from]]   <u>for</u>   an   ~~identity~~

~~management   system~~   <u>entity</u>,   the   request   containing   website   identification

15   information <u>including at least an IP address associated with the entity</u> ~~in a pre-~~

~~defined format~~; and

~~a processor for executing stored instructions to provide~~ <u>a computer-readable</u>

<u>medium   embodying   computer-readable   instructions   that   implement</u>   a

pseudonymous email address creator [[for creating]] <u>configured to:</u>

20   <u>create</u> a pseudonymous email address associated with a mail server

in response to the received pseudonymous email address generation request,

[[for associating]] <u>associate</u> the pseudonymous email address with

an email address,

[[for providing]] <u>provide</u> the created pseudonymous email address and its associated email address to the mail server associated with the pseudonymous email address,

[[for providing]] <u>provide</u> the created pseudonymous email address to the ~~identity management system~~ <u>entity;</u> and

[[for storing]] <u>store</u> the website identification information with the associated pseudonymous email address to allow centralized analysis <u>to ascertain whether the IP address is associated with a source of spam</u>.

2. (Currently Amended) The generator of claim 1 [[including]] <u>further comprising</u> a mail server interface [[for]] <u>configured to</u> [[receiving]] <u>receive</u> from the pseudonymous email address creator both the pseudonymous email address and the email address associated with the pseudonymous email address, and [[for providing]] <u>provide</u> them to the mail server associated with the pseudonymous email address ~~in a predetermined format~~.

3. (Currently Amended) The generator of claim 1 further [[including]] <u>comprising</u> a request analysis engine [[for receiving]] <u>configured to receive</u> from the request interface an indication of [[the]] <u>a</u> destination of [[the]] <u>a</u> requested alias, [[for determining]] <u>and determine</u> in accordance with the indication that the email address associated with the pseudonymous email address is a honeypot address.

4. (Currently Amended) The generator of claim 1 wherein the pseudonymous email address creator [[includes]] <u>further comprises:</u>

means for defining properties of the pseudonymous email address, the properties selected from a list including a friendly name associated with the pseudonymous email address, a management link and corresponding attachment method, and the email address the pseudonymous email address is associated with; and

<u>means</u> for providing the defined properties to [[the]] <u>an</u> associated mail server.

5.　(Currently Amended)　The generator of claim 1 further [[including]] <u>comprising</u> a rules engine [[for defining]] <u>configured to:</u>

<u>define</u> a set of routing rules in accordance with requests received by the request interface,

[[for associating]] <u>associate</u> the defined set of rules with pseudonymous email addresses generated by the pseudonymous email address creator, and

[[for providing]] <u>provide</u> the created set of rules to the mail server associated with the pseudonymous email address.

6.　(Currently Amended)　The generator of claim 5 wherein the rules engine further [[includes]] <u>comprises</u> means for defining the routing rules in accordance with a set of parameters defined in the pseudonymous email address generation request.

7.　(Currently Amended)　The generator of claim 5 wherein the rules engine further [[includes]] <u>comprises</u> means for defining the routing rules in accordance with a set of default parameters.

8.   (Original)   The generator of claim 7 wherein the default parameters are dependent upon a requester identifier associated with the pseudonymous email address generation request.

5

9.   (Canceled)

10.   (Canceled)

10   11.   (Canceled)

12.   (Canceled)

13.   (Canceled)

15

14.   (Canceled)

15.   (Canceled)

20   16.   (Canceled)

17.   (Canceled)

18.   (Canceled)

25

19.   (Canceled)

20.   (Canceled)

5   21.   (Canceled)

22.   (Canceled)

23.   (Canceled)

10
24.   (Canceled)

25.   (Canceled)

15   26.   (Canceled)

27.   (Canceled)

28.   (Canceled)

20
29.   (Canceled)

30.   (Canceled)

25   31.   (Canceled)

32.   (Canceled)

33.   (Canceled)

34.   (Canceled)

35.   (Canceled)

36.   (New) A method comprising:

receiving a request for a pseudonymous e-mail address for an entity, the request containing at least an IP address associated with the entity;

responsive to receiving the request, creating a pseudonymous e-mail address;

associating the pseudonymous e-mail address with an e-mail address;

causing communication of the pseudonymous e-mail address to the entity;

storing the IP address with the associated pseudonymous e-mail address; and

using the IP address to monitor requests for pseudonymous e-mail addresses to ascertain whether the IP address is associated with a source of spam.

37.   (New) The method of claim 36 further comprising, responsive to ascertaining that the IP address is associated with a source of spam, modifying routing rules to direct e-mail to the pseudonymous e-mail address to discard.

38.   (New) The method of claim 36 further comprising, responsive to ascertaining that the IP address is associated with a source of spam, using the pseudonymous e-mail address as a honey pot e-mail address.

39.   (New) The method of claim 36, further comprising receiving an indication that a pseudonymous e-mail address provided to a specified IP address has likely been provided to a harvesting entity.

40.   (New) The method of claim 39, further comprising responsive to receiving the indication, modifying routing rules to direct e-mail to the pseudonymous e-mail address to discard.

41.   (New) The method of claim 39 further comprising responsive to receiving the indication, using the pseudonymous e-mail address as a honey pot e-mail address.

42.   (New) The method of claim 36, wherein receiving the request comprises receiving a request from an http server.

43.   (New) The method of claim 36, wherein receiving the request comprises receiving a request from a server.

44.   (New) The method of claim 36, wherein receiving the request comprises receiving a request from a user.

45. (New) The method of claim 36, wherein the creating a pseudonymous e-mail address is performed automatically and without input from a user as to content of the pseudonymous e-mail address.

46. (New) The method of claim 36, wherein the creating a pseudonymous e-mail address is performed automatically responsive to a click on a contact link.

47. (New) A tangible computer-readable medium having stored thereon, computer-executable instructions that, if executed by a computing device, cause the computing device to perform a method comprising:

receiving a request for a pseudonymous e-mail address for an entity, the request containing at least an IP address associated with the entity;

responsive to receiving the request, creating a pseudonymous e-mail address;

associating the pseudonymous e-mail address with an e-mail address;

causing communication of the pseudonymous e-mail address to the entity;

storing the IP address with the associated pseudonymous e-mail address; and

using the IP address to monitor requests for pseudonymous e-mail addresses to ascertain whether the IP address is associated with a source of spam.

48. (New) The tangible computer-readable medium of claim 47 further comprising computer-executable instructions that, if executed by the computing device, cause the computing device to perform a method further comprising

responsive to ascertaining that the IP address is associated with a source of spam, modifying routing rules to direct e-mail to the pseudonymous e-mail address to discard.

5   49.   (New) The tangible computer-readable medium of claim 47 further comprising computer-executable instructions that, if executed by the computing device, cause the computing device to perform a method further comprising, responsive to ascertaining that the IP address is associated with a source of spam, using the pseudonymous e-mail address as a honey pot e-mail address.

10

       50.   (New) The tangible computer-readable medium of claim 47 further comprising computer-executable instructions that, if executed by the computing device, cause the computing device to perform a method further comprising receiving an indication that a pseudonymous e-mail address provided to a

15   specified IP address has likely been provided to a harvesting entity.

       51.   (New) The tangible computer-readable medium of claim 50 further comprising computer-executable instructions that, if executed by the computing device, cause the computing device to perform a method further comprising

20   responsive to receiving the indication, modifying routing rules to direct e-mail to the pseudonymous e-mail address to discard.

       52.   (New) The tangible computer-readable medium of claim 50 further comprising computer-executable instructions that, if executed by the computing

25   device, cause the computing device to perform a method further comprising

responsive to receiving the indication, using the pseudonymous e-mail address as a honey pot e-mail address.

53.   (New)   The tangible computer-readable medium of claim 47, wherein receiving the request comprises receiving a request from an http server.

54.   (New)   The tangible computer-readable medium of claim 47, wherein receiving the request comprises receiving a request from a server.

55.   (New)   The tangible computer-readable medium of claim 47, wherein receiving the request comprises receiving a request from a user.

56.   (New)   The tangible computer-readable medium of claim 47, wherein the creating a pseudonymous e-mail address is performed automatically and without input from a user as to content of the pseudonymous e-mail address.

57.   (New)   The tangible computer-readable medium of claim 47, wherein the creating a pseudonymous e-mail address is performed automatically responsive to a click on a contact link.

58.   (New) A system comprising:

means for receiving a request for a pseudonymous e-mail address for an entity, the request containing at least an IP address associated with the entity;

means for responsive to receiving the request, creating a pseudonymous e-mail address;

means for associating the pseudonymous e-mail address with an e-mail address;

means for causing communication of the pseudonymous e-mail address to the entity;

means for storing the IP address with the associated pseudonymous e-mail address; and

means for using the IP address to monitor requests for pseudonymous e-mail addresses to ascertain whether the IP address is associated with a source of spam.